



Department of Homeland Security Daily Open Source Infrastructure Report for 20 October 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- Alaska Governor Frank Murkowski has directed the Department of Environmental Conservation to assemble an Arctic Pipeline Technology Team and called for a corrosion conference to improve pipeline integrity. (See item [1](#))
- Reuters reports flu vaccine makers will provide 115 million doses to the U.S. market this year, by far the most ever, but problems with distribution mean it may still be difficult to get a shot. (See item [29](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *October 18, Manufacturing.net* — **Alaska Governor announces measures to ensure pipeline integrity.** Alaska Governor Frank Murkowski has directed the Department of Environmental Conservation (DEC) to assemble an Arctic Pipeline Technology Team and called for a corrosion conference to improve pipeline integrity. The team will be created by a Memorandum of Understanding between the DEC, the Department of Natural Resources, the Alaska Oil and Gas Conservation Commission, and the Federal Office of Pipeline Safety. The team will share information on preserving pipeline integrity in arctic and sub-arctic climates, as well as troubleshooting design, construction, operation, and maintenance problems as a way to confirm

the correct technology is applied to the North Slope pipeline system.

Source: <http://www.manufacturing.net/article/CA6382363.html>

2. *October 18, Access North Georgia* — **Georgia gas station caught earlier this year for water laced gasoline.** The state Agriculture Commissioners office said Wednesday, October 18, that the Cumming gas station caught with water in it's gasoline was cited earlier in the year for the same thing. Tommy Irvin confirms inspectors found water in the gasoline in all pumps selling regular unleaded at the Racetrac on Buford Highway. Irvin says, "A stop-sale order was issued and the nozzles on 18 pumps dispensing regular gasoline were sealed. They will remain locked until we are convinced — and laboratory tests confirm — there is no water in the pumps, lines or storage tanks." Earlier this year, agriculture officials found water in the gas. Officials speculate that rain water seeped into an underground storage causing the incident.

Source: http://www.accessnorthga.com/news/hall/newfullstory.asp?ID=1_08042

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

3. *October 19, Mercury News (CA)* — **Residents evacuated, major connector route closed following big-rig collision in California.** Pacheco Pass was closed for hours and some nearby residents were evacuated Thursday morning, October 19, after two big-rigs collided, sending hazardous chemicals across Highway 152 near Gilroy, CA. A refrigerator truck and a truck carrying an unknown corrosive flammable chemical collided shortly after 7 a.m. PDT Thursday near Bloomfield Avenue, just east of Gilroy. The road was closed in both directions. One of the trucks was carrying 55-gallon barrels of a sulfuric acid solution and a hydrogen peroxide solution, 750 pounds of potassium nitrate and an unknown flammable substance. The truck had a total of a dozen barrels in its trailer, but it was not known how many were filled with sulfuric acid and how many with hydrogen peroxide. A barrier was also set up for a mile around the spill as a precaution. A temporary flight restriction was filed to keep helicopters and small planes away from the site as a precaution.

Source: <http://www.mercurynews.com/mld/mercurynews/news/15798213.htm>

[\[Return to top\]](#)

Defense Industrial Base Sector

4. *October 18, CongressDaily* — **Defense official pledges continued investments in special operations.** Despite growing concerns across the military services about increasingly strained Defense budgets in fiscal 2008 and beyond, a senior Department of Defense official on Wednesday, October 18, said the military has all the money it needs to make planned investments in U.S. special operations forces. Indeed, the military will have enough money to grow its special forces by 15 percent, while also equipping them with new technologies needed for the war on terror, said Mario Mancuso, deputy assistant secretary of Defense for special operations and combating terrorism. Speaking at a breakfast meeting with reporters, Mancuso said Pentagon officials took into account a flattening of defense dollars when they spelled out their goals and strategy for special forces in the Quadrennial Defense Review (QDR). As such,

they placed an emphasis on technology and other investments with a high rate of return for use against both state and non-state adversaries. Special forces are expanding their abilities to fight "irregular warfare" as spelled out in the QDR, essentially battling insurgents and other unconventional enemies, Mancuso said. Doing so involves investing in satellites and other intelligence and reconnaissance systems that allow special operations troops to conduct protracted surveillance missions.

Source: http://www.govexec.com/story_page.cfm?articleid=35296&dcn=to_daysnews

[[Return to top](#)]

Banking and Finance Sector

5. *October 18, Reuters* — **FBI, police crack Colombian money laundering ring.** U.S. authorities cracked a multimillion-dollar international money-laundering ring on Wednesday, October 18, with the arrest of 26 people in Colombia, Florida, and New York. More than \$10 million in drug money and \$6.5 million in narcotics were seized, according to the FBI, the U.S. Drug Enforcement Administration, and the New York Police Department. Authorities said the group was laundering money through a sophisticated black market peso exchange. The exchange involved "peso brokers" who acted as middle men between drug traffickers, who wanted to launder drug profits, and Colombian companies and individuals, who wanted to buy U.S. dollars but avoid paying Colombian taxes, import duties, and transaction fees.
Source: http://news.yahoo.com/s/nm/20061018/ts_nm/crime_usa_colombia_dc_1
6. *October 18, Pretoria News (South Africa)* — **ATM bombers in terrorist onslaught.** A gang of explosives experts may be responsible for blowing up a Standard Bank ATM outside Krugersdorp, South Africa, on Tuesday, October 17. The gang, which has also attacked teller machines belonging to Absa and FNB, may be employing dozens of explosive technicians to destroy ATMs and retail business strong rooms. The latest attack brought the number of ATMs destroyed in the past two years to 17 and it was the 43rd such attack in the past 24 months. Although no money was taken in Tuesday's attack, thousands of dollars of damage was caused to the ATM machine. The Consumer Goods Council of South Africa said the gang had also been responsible for attacks — described by Absa as a "terrorist onslaught" — on PEP, Spar, Checkers and Metro Cash and Carry stores throughout the country. Police teams investigating the attacks say the syndicate puts its "operatives" on public buses with explosive-laden suitcases. A police explosives expert said the explosive used was usually ammonium nitrate, which was probably stolen from mines. The modus operandi, said the police officer, showed that the robbers choose very specific targets, and they know exactly how much explosive to use to blow up their targets.
Source: http://www.int.iol.co.za/index.php?from=rss_News&set_id=1&click_id=&art_id=vn20061018030712415C151358
7. *October 18, CBC News (Canada)* — **Police uncover debit-card skimming at Calgary gas station.** Calgary police have charged three men in connection with a debit-card skimming operation at a gas station. Det. Colin Harper says debit-card skimming operations are becoming more common in the city. In some cases criminals set up pin hole cameras and DVD recorders in stores to track customers' key strokes when they use their bank cards, he said. Other times they insert an extra computer chip into the store's debit card reader. The

information collected is then used to create counterfeit cards. Harper says police believe the three men arrested this week are linked to other similar debit-skimming operations in the city. Police also believe the suspects are connected to a counterfeit bank-card ring based in Ontario and Quebec.

Source: <http://www.cbc.ca/canada/calgary/story/2006/10/18/skimming-cards.html?ref=rss>

8. *October 18, CSO Online* — **New phishing attack uses fake journalists to target bank workers.** Hundreds of bank employees at a mid-size bank — as well as other banks — have received personally addressed e-mails purporting to be from a journalist who is doing a follow up story on a recent leak of customer records from the bank. The journalist writes that he saw the employee's name in an article from a news site and would like to interview the employee for a follow-up piece. The e-mail then provides what appears to be a link to the Central News story — a URL that includes the bank's name in its characters. The e-mail contains a keylogging bot from a Chinese Website that store all of the employee's keystrokes. The eventual goal of such a targeted attack would be to have a bank employee with deep access to accounts and account information unwittingly log passwords and account information, which the bot would deliver back to the attacker. A query of an online discussion board by the bank's CSO, where someone received precisely the same message, showed the scam had also occurred at another bank.

Source: http://www2.csoononline.com/blog_view.html?CID=25905

9. *October 18, ComputerWeekly* — **Data center outage at HSBC crashes card system.** HSBC has confirmed that an outage at its data center on Sunday, October 15, stopped thousands of customers using their cash cards. The crash brought down services for three hours when problems with the system's communication with card reading devices prevented transactions at ATM cash machines or shops being authorized. HSBC said the bank did not know why the problem had arisen and was still investigating to determine the cause. Not all transactions were affected, with problems concentrated in the South and South West of England and worsening as demand on the system increased during the afternoon. A spokesperson said, "There were no problems with security or fraud, simply an unfortunate and very rare systems error."

Source: <http://www.computerweekly.com/Articles/Article.aspx?liArticleID=219229&PrinterFriendly=true>

10. *October 18, Canadian Press* — **Identity theft threatens the future of e-commerce, experts warn.** A complete overhaul of the way identity is verified on the Internet is the only way to stem the exponentially growing problem of online fraud. Ontario's privacy commissioner said increasingly sophisticated Internet scammers are threatening to make the way people use the Internet obsolete. "With the exponential growth of on-line fraud, phishing, pharming (and) identity theft, the existing identity infrastructure of the Internet is simply no longer sustainable," Anne Cavoukian said. Cavoukian teamed up with Microsoft executives at a news conference in Toronto to discuss why the Internet is so desperately in need of a change. The group suggested using "infocards," which would enable Websites to verify a customer's identity without receiving or keeping personal or financial information, much like the cards people carry in their wallets. Infocards would allow a bank to act as a middleman in an on-line purchase, sending payment confirmation to a retailer without transmitting a credit card number. Chief Microsoft identity architect Kim Cameron says the infocards must "work across Microsoft, Linux, Apple, every possible permutation and combination. It has to work on computers, it has to work on cell

phones, so it's really a very all-embracing thing."

Source: http://www.globeinvestor.com/servlet/story/RTGAM.20061018.wp_rivacy18/GIStory/

11. *October 18, SC Magazine* — Identity thieves use Yahoo e-mail to purchase goods online.

Over three quarters of suspected identity thefts use Yahoo e-mail accounts, according to a report published Tuesday, October 17. The research, completed by checkmyfile.com, found that consumers using popular Internet based email addresses, such as Yahoo and Hotmail, to make online purchases are more likely to be blacklisted as identity thieves by retailers. It found that companies accepting transactions from such e-mail accounts are up to seven times more likely to have to refund a consumer's credit card because the card owner doesn't recognize the purchase, compared to customers using other e-mail providers. According to the report 82 percent of suspected identity theft attempts use Yahoo addresses. Barry Stamp of checkmyfile.com said, "A Yahoo email address appears to be the weapon of choice for the professional identity thief, because the user of the address is untraceable in most cases. Yahoo is also very popular and has a good name for reliability — an ideal thing to hide behind for identity thieves," he said.

Source: <http://www.scmagazine.com/uk/news/article/599320/identity-thieves-use-yahoo-email-purchase-goods-online/>

[\[Return to top\]](#)

Transportation and Border Security Sector

12. *October 19, Associated Press* — American jet makes emergency landing at JFK.

An American Airlines jet from Dallas landed safely at John F. Kennedy International Airport (JFK) on Thursday, October 19, after an indicator light went off in the cockpit, the airline said. The American Airlines Flight 704 departed from the Dallas-Fort Worth International Airport and was due to land at LaGuardia Airport at 12:10 p.m. EDT, said airline spokesperson Tim Wagner. "The captain got an indication that there was a mechanical issue with one of the wings," Wagner said. The flight was carrying 139 passengers and five crewmembers, Wagner said.

Source: http://wcbstv.com/topstories/local_story_292133547.html

13. *October 19, Spokesman Review (WA)* — Faulty ties blamed for Amtrak derailment.

The National Transportation Safety Board (NTSB) reported Wednesday, October 18, that improper track maintenance and inadequate federal standards are to blame for an Amtrak derailment last year near Home Valley, WA. That April 3, 2005, derailment of Amtrak's Empire Builder train injured 30 of the 115 people on the train as it headed from Spokane, WA, toward Portland, OR. The train was traveling on BNSF Railway Co. tracks. The NTSB said that BNSF failed to respond to multiple reports about rough conditions on that segment of track. That roughness was caused by the failure of concrete crossties, which ultimately abraded to the point that they allowed the rails to bend and the train's wheels to drop between them. As a result, the NTSB recommended that the Federal Railroad Administration extend its safety standards where trains travel at slower speeds.

Source: <http://www.spokesmanreview.com/local/story.asp?ID=155309>

14. *October 18, USA TODAY* — **Airlines are making profits.** The U.S.'s airlines are about to do something they haven't done in six years: report profits for a second—consecutive quarter. Fort Worth—based American Airlines is expected to report a profit despite costs associated with the August 11 bomb—plot scare in London. The largest U.S. carrier in the U.S.—UK market, American said last month that the terrorist scare and its aftermath cost about \$50 million in lost revenue. Two other big, Texas—based carriers, Continental in Houston and Southwest in Dallas are expected to report quarterly profits on Thursday, October 19, 2006. The rest of the big airlines are expected to report profits over the next few weeks. The only exceptions will be Delta and Northwest, both of which have been operating in Chapter 11 bankruptcy since September 2005. And even they are expected to report third—quarter operating profits excluding bankruptcy—related costs. Last achieved in the second and third quarters of 2000, the latest run of profitability for the industry is driven by general economic strength, high travel demand, and higher fares.

Source: http://www.usatoday.com/travel/flights/2006-10-18-air-profit-s-usat_x.htm

15. *October 17, Department of Transportation* — **FMCSA public listening session.** The Federal Motor Carrier Safety Administration (FMCSA), looking to improve the way it monitors and assesses the safety performance of the rapidly growing commercial vehicle industry, is developing a new approach that focuses on interacting with more carriers on a regular basis through its Comprehensive Safety Analysis 2010 initiative (CSA 2010). A public listening session to obtain feedback on the latest progress of the initiative will be held in Washington, DC, on November 16, 2006. A Federal Register notice summarizing the safety initiative and announcing the listening session was published in the Federal Register on Tuesday, October 17, 2006. Comments can be submitted online at the Department of Transportation's Docket Management System at <http://dmses.dot.gov>. Reference document number FMCSA-2004-18898.

Source: <http://www.dot.gov/affairs/fmcsa0606.htm>

16. *October 17, GovExec* — **Immigration, customs agency headed for hiring spree.** The Immigration and Customs Enforcement (ICE) agency is planning to hire 2,000 agents to work at its division responsible for detaining illegal aliens and sending them out of the United States when possible. Stephen Dade, Pacific Rim regional director for the Federal Protective Service, which also is within ICE, told about 130 employees in an e-mail memorandum Sunday, October 15, that "2,000 openings in [ICE's Office of] Detention and Removal [Operations] would be available soon." If 2,000 agents are hired, ICE would grow by more than 13 percent, to about 17,000 employees from 15,000. ICE is the Homeland Security Department's largest investigative branch and has four main divisions, including FPS, which is responsible for securing the more than 8,800 federal facilities nationwide. Dade said the positions will be listed at <http://www.usajobs.gov>

Source: http://www.govexec.com/story_page.cfm?articleid=35279&dcn=to_daysnews

[[Return to top](#)]

Postal and Shipping Sector

17. *October 18, Associated Press* — **White substance in envelope creates scare in central Maine town.** A white substance that turned out to be paper dust set off a scare on Tuesday, October

17, that resulted in dozens of emergency responders descending on a home where a woman reported being burned by the material. Police and fire officials received a call late Tuesday morning from a home in the village of Shawmut, ME, where Grace MacKenzie reported opening her Central Maine Power (CMP) electric bill and experiencing a burning and numbing sensation on her hands from a powdery material. Hazardous material response units were dispatched to the home where they set up trucks and decontamination equipment. The area was blocked off to traffic, the powder was taken to a state laboratory in Augusta for testing, and the village post office was shut down. In the end it was determined that the material in question was paper dust that sometimes accumulates in CMP bills, said Police Chief John Emery. Waterville fire Capt. David LaFountain said, "My guess is that she was exposed to a chemical before she opened the letter and that caused the problem," he said.

Source: http://www.boston.com/news/local/maine/articles/2006/10/18/wite_substance_in_envelope_creates_scare_in_central_maine_to_wn/

18. *October 17, Beacon News (IL)* — **Third mail scare again causes no injuries.** For the third time in just over six weeks, an envelope containing a suspicious-looking powder has been found in a bill-processing center in Naperville, IL. A five-member Naperville Fire Department crew was dispatched at 6:31 p.m. Sunday, October 15, to the billing center at 2012 Corporate Lane, after employees discovered an envelope that "apparently had a suspicious substance coming out of it," Assistant Fire Chief Mike Zywanski confirmed Monday, October 16. Crewmembers performed two tests at the scene on the powder, which had "a positive reading for protein," Zywanski said. Protein also is found in anthrax, a potentially lethal bacterium enclosed five years ago in a number of letters that were mailed up and down the East Coast. The tests ultimately showed the powder to be a harmless mixture of green dye and holmium sulfate, the latter of which is used in ceramics and glass-making. No one was injured in Sunday's incident or in two earlier ones August 30 and September 13 at the processing center. Source: http://www.suburbanchicagonews.com/beaconnews/news/99159.2_1_AU17_POWDER_S1.article

[[Return to top](#)]

Agriculture Sector

19. *October 19, Dow Jones* — **Soybean rust marches into Arkansas, Indiana, Virginia.** Asian soybean rust has been found in Virginia, Arkansas, and Indiana, bringing the total number of counties found to be infected with the plant disease to 158, in 15 U.S. states. The airborne fungus has moved rapidly from the Deep South into the heart of the Corn Belt during the past week, and is now found as far north as Knox County, IN. "Perhaps the most important thing we have learned from the appearance of soybean rust in Kentucky, Illinois and Indiana is that southerly winds can carry spores long distances," said Purdue University plant pathologist Greg Shaner. Although the Wednesday, October 18 discovery was the first ever found in Indiana, Shaner says the airborne fungus poses no threat to the 2006 Indiana soybean harvest, as more than 90 percent of the crop has already been picked or reached physiological maturity. This week's Indiana outbreaks likely originated from spores from infected fields in western Kentucky and southeastern Illinois. Soybean rust has most recently also been reported in seven counties of eastern Arkansas — Ashley, Chicot, Desha, Jefferson, Lincoln, Lonoke, and Prairie — and in Suffolk and Chesapeake Counties of southeastern Virginia as well.

Source: <http://www.cattlenetwork.com/content.asp?contentid=77460>

20. *October 19, Farm Press* — **Study shows impact of ag policy reform.** U.S. farm policy reform without corresponding multilateral trade reform and market access would result in lower production and incomes for many U.S. agricultural producers over the next 15 years, according to a study conducted by the Australian Bureau of Agricultural and Research Economics. Among the program crops, the largest reductions in production would occur for cotton and rice, which would decline by 11 percent and 13 percent respectively by 2020 if the U.S. undertook reform alone. Soybeans, corn, and wheat would incur relatively small declines in production by 2020, just under one percent for soybeans and around three percent for wheat and corn, due to lower current levels of support for these commodities compared with rice or cotton. As corn prices rise, it is likely that livestock producers would increase their demand for other feed grains that can be used as livestock feed rations. The resulting higher prices for other feed grains may lead to acreage shifts out of other crops, particularly soybeans, rice and cotton. U.S. consumers would then be paying higher prices, not just for products derived from grains, such as high fructose sweeteners, but for soybeans, rice and cotton as well.

Study: http://www.abareconomics.com/publications_html/trade/trade_06/us_ag.pdf

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

21. *October 19, Associated Press* — **UN reports growing number of ocean dead zones.** The number of oxygen-starved "dead zones" in the world's seas and oceans has risen more than a third in the past two years because of fertilizer, sewage, animal waste, and fossil-fuel burning, United Nations experts said Thursday, October 19. Their number has jumped to about 200, according to new estimates released by UN marine experts meeting in Beijing. In 2004, UN experts put the estimate at 149 globally. The damage is caused by explosive blooms of tiny plants known as phytoplankton, which die and sink to the bottom, and then are eaten by bacteria which use up the oxygen in the water. Those blooms are triggered by too many nutrients — particularly phosphorous and nitrogen. Oxygen starvation robs the seas and oceans of many fish, oysters, sea grass beds and other marine life — and the number of such dead zones has grown every decade since the 1970s. All the dead zones pose a danger to global fish stocks, which many marine scientists say are increasingly hammered by overfishing and pollution.

Source: <http://www.nola.com/newsflash/louisiana/index.ssf?/base/news-28/1161275643141740.xml&storylist=louisiana>

22. *October 19, Food Production Daily (Europe)* — **Phage product found effective against Listeria.** A dose of bacteriophages can help ready-to-eat meat producing companies meet food safety standards for Listeria, according to a university study. To food pathogens like Listeria, bacteriophages are the viral hit squads of the microscopic world. Bacteriophages are viruses that target bacteria, rather than human, plant or animal cells. They have the potential to be the next big technological advance in anti-bacterial agents processors can use in ensuring their products do not leave the plant loaded with dangerous pathogens like Listeria, Salmonella, Campylobacter, and E. coli. The study was done by Lieve Vermeiren of Belgium-based Gent University's department of food safety and food quality. The bacterium regularly causes serious food poisoning. The concern for this pathogen results from its ability to cause listeriosis in humans, a condition known for its 30 percent mortality rate.

Source: <http://www.foodproductiondaily.com/news/ng.asp?n=71423-ebi-b>

[[Return to top](#)]

Food Sector

23. *October 19, Agricultural Research Service* — **Food poisoning bacterium's genetic structure probed.** Inner workings of a food–poisoning organism called *Campylobacter lari* have been uncovered in greater detail than ever before by Agricultural Research Service (ARS) scientists in California. Their forays into the genetic makeup, or genome, of this little–known pathogen reveal new details about the structure, or sequence, of its genes. *C. lari* is a cousin of the better–known *C. jejuni*, another "bad–guy" bacterium. *C. jejuni* causes millions of cases of diarrhea every year, according to microbiologist William G. Miller of ARS' Produce Safety and Microbiology Research Unit. Food poisoning outbreaks occurring in some other countries have been attributed to *C. lari* and have attracted the attention of U.S. food safety researchers and public health professionals. Similarities and differences among these genomes will provide important clues to how *Campylobacter* successfully infects us, which may lead to new tactics to outmaneuver the genes that orchestrate infection.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

[[Return to top](#)]

Water Sector

24. *October 19, CanWest News Service* — **New law to protect Ontario drinking water.** Communities throughout Ontario, Canada, will be required to identify and eliminate any significant risks to their water supplies under the terms of a new Clean Water Act passed Wednesday, October 18, in the Ontario legislature. Environment Minister Laurel Broten said the act delivered on 12 of the recommendations that came out of the inquiry into the Walkerton, Ontario, tainted water tragedy. In May 2000, seven people in Walkerton died after *E. coli* tainted the water. One of the key recommendations was that drinking water sources should be protected by developing watershed–based source protection plans for all of Ontario's watersheds. Environmental groups heaped praise on the provincial government for bringing in the legislation, which lays out a formal process for identifying threats to drinking water sources and requires the establishment of local committees to address the threats. Broten said the government has provided \$7 million for water source protection measures that have already been identified and has given local conservation authorities \$120 million to identify how much water there is, how safe it is and what the risks are to it.

Source: <http://www.canada.com/ottawacitizen/news/story.html?id=c10320aa-aeb1-4149-9d24-61fc205a1334&k=4171>

25. *October 19, WIFR (IL)* — **Hundreds of Roscoe, Illinois, water wells could be contaminated.** When it rains in Roscoe, IL, sandy soil lets the water flow all the way down into the water table, which is where people with wells get their drinking water. On Wednesday, October 18, 370 people in Roscoe found out what else is leaking into the water with the rain. A chemical used for dry cleaning and metal degreasing has been found in two water wells in Roscoe. Those

using city water are not affected. The chemical known as PCE is suspected to cause cancer. The tainted water contained over double the concentration of PCE allowed by the EPE, but negative health effects are only anticipated when very high levels of PCE are present for an extended period of time. Those who live in the affected area can pick up a testing kit at the Roscoe Township Office.

Source: <http://www.wifr.com/home/headlines/4430991.html>

26. *October 19, Tri-Town News (NJ)* — **Water rate will increase 79 percent in Howell.** Barring any further legal action, Howell, NJ, customers of the Parkway Water Co. will see their water rate rise about 79 percent, according to state Board of Public Utilities spokesperson Eric Hartsfield. Hartsfield said the average Parkway Water customer should expect to see his annual water bill rise to about \$525, up from \$294. Parkway Water officials have previously said the higher rates are needed as the firm continues to buy water from other sources in order to serve its customers in Howell. A deal to sell the water company and its customer base in Howell to the Brick Township Municipal Utilities Authority fell apart over possible future litigation stemming from radium contamination in wells that Parkway Water had been dealing with over the past three years.

Source: http://tritown.gmnews.com/news/2006/1019/Front_Page/043.html

27. *October 19, USA TODAY* — **Vegas reaching for rural water.** The Southern Nevada Water Authority wants to pump vast quantities of groundwater from rural eastern Nevada valleys and pipe it 250 miles south to Las Vegas, the nation's fastest-growing major metro area, a tourist haven with a limited water supply strained by population and prolonged drought. The authority built a computer model to predict effects on the water table but didn't run it. When it was run by a National Park Service hydrologist, it showed a 150-foot drop over 75 years. After hearings last month, a decision rests with State Engineer Tracy Taylor. More hearings on plans in other valleys are pending. The water authority aims to build a pipeline by 2015 and pump nearly 30 million gallons a year from 19 wells in Spring Valley alone. At stake, ranchers say, are livelihoods and a delicate ecological balance on a landscape cursed with at most eight inches of rain and snow a year. Since early settlers, water has been the West's scarcest and most valuable resource. Rivers, lakes, and streams have been dammed, drained, and diverted for decades and now offer little extra supply for expanding urban centers such as Salt Lake City, El Paso, Albuquerque, Phoenix, and Tucson.

Source: http://www.usatoday.com/news/nation/2006-10-18-vegas_x.htm

[\[Return to top\]](#)

Public Health Sector

28. *October 19, Reuters* — **FDA accelerates approval process for some generic drugs.** The Food and Drug Administration (FDA) will accelerate its reviews of certain generic drugs, a top agency official said Wednesday, October 18, a move the industry said could help get some cheaper alternatives on the market sooner. Companies will be given priority if their application is the first one proposing a generic version of a brand-name drug that is no longer protected by a patent or market exclusivity, said Dr. Steven Galson, director of the FDA's Center for Drug Evaluation and Research. Generic medicines that would address a public health emergency or nationwide shortage will also see faster reviews, he said. The FDA has a backlog of more than

800 generic drugs awaiting approval under the current process that evaluates all applications in the order it receives them. In 2005, the median time for an approval was more than 16 months, according to the FDA.

Source: <http://www.latimes.com/business/la-fi-generic19oct19.1.7134240.story>

29. *October 19, Reuters* — **U.S. to get 115 million flu vaccines this year.** Flu vaccine makers will provide 115 million doses to the U.S. market this year, by far the most ever, but vexing distribution problems mean it may still be difficult to get a shot, health officials said on Wednesday, October 18. Doctors should start vaccinating patients as soon as they receive their vaccine orders, the U.S. Centers for Disease Control and Prevention (CDC) said. Dr. Jeanne Santoli, deputy director of the CDC's Immunization Services Division, told reporters that 40 million doses had arrived at either distributors or doctors' offices from the manufacturers, and estimated that 75 million doses would arrive by the end of October. The flu season peaks in February or later in the United States, so there is plenty of time to be vaccinated, she said. Last year, 81.2 million doses of vaccine were available and a few went unused. Earlier this week Sanofi Pasteur said its flu shots specially formulated for young children would be delayed and that many doses would not be available until November.

Source: http://today.reuters.com/news/articlenews.aspx?type=healthNews&storyID=2006-10-19T132116Z_01_N18370442_RTRUKOC_0_US-FLU.xml

30. *October 17, Associated Press* — **Study finds a widespread risk of reactions to some medicines.** Harmful reactions to medicines, usually attributed to accidental overdoses and allergic reactions, send more than 700,000 Americans to emergency rooms each year, government research shows. The results, from 2004–5, represent the first two years of data from a national surveillance project on outpatient drug safety. The project was developed by the federal Centers for Disease Control and Prevention, the Food and Drug Administration and the United States Consumer Product Safety Commission. The study was published Wednesday, October 18, in the Journal of the American Medical Association. The medicines most commonly implicated in the reactions included insulin for diabetes; warfarin, an anticoagulant, and amoxicillin, an antibiotic used for many infections. People 65 and older faced more than double the risk of requiring emergency room treatment and were nearly seven times more likely to be admitted to the hospital than younger patients. Journal abstract:

<http://jama.ama-assn.org/cgi/content/abstract/296/15/1858>

Source: http://www.nytimes.com/2006/10/18/health/18drug.html?_r=1&ref=health&oref=login

[[Return to top](#)]

Government Sector

Nothing to report.

[[Return to top](#)]

Emergency Services Sector

31.

October 19, Government Technology — **San Francisco takes steps to improve emergency management, ensure safety.** On Tuesday, October 17, San Francisco Mayor Gavin Newsom announced the launch of AlertSF, a new aspect of the Emergency Alert system which sends text message alerts to mobile devices. Along with this, San Francisco's Disaster Council will be reviewing the Earthquake Response Plan Enhancement. This Enhancement supplements the city's existing Emergency Operations Plan with catastrophic–earthquake specific response planning, input from all city departments, and data gathered from past urban earthquakes around the world. To prepare this Enhancement, the San Francisco Office of Emergency Services and Homeland Security reviewed extensive research of after–action reports and lessons learned from large urban earthquakes, including, Loma Prieta, the Northridge earthquake of 1994, and the Hanshin–Awaji earthquakes in Japan in 1995. They used this data to identify challenges to earthquake response and disaster management. On Thursday, October 19, Newsom and Acting Director Amy Lee announced the formation of a new management unit — the Structural Safety and Emergency Management Division (SSEM) — within the city's Department of Building Inspection. The SSEM Division will implement new seismic safety programs, including the proposed automatic gas shut–off valve, the seismic risk reduction of soft/weak–story, open–front wood–frame buildings and the Pacific Earthquake Engineering Research Center Tall Buildings Initiative.

Source: <http://www.govtech.net/news/news.php?id=101763>

32. *October 18, International Hurricane Research Center* — **Hurricane center identifies ten most hurricane vulnerable areas.** The entire East and Gulf Coasts are subject to hurricane impacts, but some areas are much more vulnerable than others. Dr. Stephen P. Leatherman, Director of the International Hurricane Research Center, has released a list titled “10 Most Vulnerable U.S. Mainland Areas to Hurricanes.” New Orleans tops the list with the protective levees of this below–sea level city being in little better shape than when Hurricane Katrina flooded 80 percent of the city last year. Twelve criteria were used to evaluate the vulnerability of U.S. mainland areas to hurricanes. Cyclonic energy (hurricane frequency and storm intensity) and levee/dike failure were primary determinants of vulnerability. Physical factors included storm surge and freshwater flooding potential as well as coastal erosion trends and island breaching history. Socioeconomic indicators involved populations at risk, evacuation distance and routes, what’s at risk, and local/state capabilities to respond to major hurricane impacts. Florida dominates the list with four out of the ten most vulnerable areas, but this is to be expected with its long shoreline that includes both the Atlantic and Gulf Coasts.

Source: http://www.ihrf.fiu.edu/media/docs/10_Most_Hurricane_Vulnerable_Areas.pdf

[[Return to top](#)]

Information Technology and Telecommunications Sector

33. *October 19, IDG News Service* — **First security flaw signaled in IE7.** Less than 24 hours after the launch of Internet Explorer 7 (IE7), security researchers are poking holes in the new browser. Danish security company Secunia reported Thursday, October 19, that IE7 contains an information disclosure vulnerability, the same one it reported in IE6 in April. The vulnerability affects the final version of IE7 running on Windows XP with Service Pack 2. If a surfer uses IE7 to visit a maliciously crafted Website, that site could exploit the security flaw to read information from a separate, secure site to which the surfer is logged in. Secunia rates the

security flaw as "less critical," its second-lowest rating, and suggests disabling active scripting support to protect the computer.

Secunia advisory: <http://secunia.com/advisories/22477>

Source: http://www.infoworld.com/article/06/10/19/HNie7securityflaw_1.html

34. *October 19, CNET News* — Cybercrooks shift towards new Web-based techniques.

Cybercrooks are moving to new Web-based techniques to control the machines they have commandeered, popularly referred to as "zombies." Before, they used to send orders via Internet chat services, but with that method, they ran the risk of inadvertently revealing the location of the zombies and themselves. The change in tactics makes it harder to identify zombies on a network, and it becomes tougher for security professionals to use the hackers' own tools to spy on them. In addition, the switch to Web-based control increases the threat of zombies to enterprises and other organizations, as that method can't be blocked as easily as the previous technique.

Source: http://news.com.com/Zombies+try+to+blend+in+with+the+crowd/2100-7349_3-6127304.html?tag=nefd.lede

35. *October 19, Sophos* — Trojan horse tempts users with pictures of Russian pop group.

Sophos has warned of a new spyware Trojan horse offering pictures and intimate details about the personal lives of the infamous Russian pop group t.A.t.U. The Troj/Banito-BE Trojan horse has been spammed out to e-mail users around the world in a message with the subject line "Photos of TATU." It attempts to entice recipients into clicking on a malicious attachment purporting to contain photos and gossip about the controversial duo, who first sprang to fame in 2003. The e-mails have three files attached: tatu_1.jpg and tatu_2.jpg are promotional images of the duo, but TATU.CHM is a malicious compressed HTML help file which as well as offering an album of images of the notorious Eurovision entrants also gives hackers access to the innocent user's PC in order to spy, steal or cause havoc.

Source: <http://www.sophos.com/pressoffice/news/articles/2006/10/tatu.html>

36. *October 18, eWeek* — Microsoft releases IE7 as free download. Microsoft made the newest upgrade for its Web browser, Internet Explorer 7 (IE7) for Windows XP, available for download Wednesday, October 18. The browser, which can be downloaded at no cost, is currently available only in English and runs on Windows XP Service Pack 2, Windows XP 64-bit Edition and Windows Server 2003 Service Pack 1. IE7 for XP will be made available in 23 Windows-supported languages over the coming weeks, said Gary Schare, director of Windows product management. Microsoft is also offering unlimited free phone support to consumers in North America who decide to run IE7. This support will be extended as additional languages are released, he said.

IE7 download: <http://www.microsoft.com/windows/ie/default.msp>

Source: <http://www.eweek.com/article2/0.1895.2032804.00.asp>

37. *October 18, eWeek* — Today's NAC remains vulnerable to attack. According to the latest figures from Forrester Research, some 40 percent of all enterprises in North America will have some form of Network Admission Control (NAC) in place by the end of 2006. However, industry experts say the tools are far from complete and, by themselves, do not yet provide an adequate level of security for companies to depend on. The most outspoken critic of NAC security has been Ofir Arkin, chief technology officer of Insightix, based in Ra'anana, Israel.

Arkin maintains that, despite his public warnings and other software vendors' concessions that NAC is not yet foolproof, many companies are adopting the technologies without understanding the risks involved. Arkin has outlined a series of weaknesses that he believes exist in current NAC installations. Among those vulnerabilities is the ability for outsiders to dupe NAC systems' so-called IP sniffers, which are used to scan data packets passing through the products' monitoring tools to validate information about devices connecting to a network. Common loopholes that let devices communicate inside their network segment without sending IP traffic through a monitoring point could allow for virus infections or for a device to gain access to unauthorized areas of a company's network, Arkin contends.

Source: <http://www.eweek.com/article2/0,1895,2029790,00.asp>

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	6346 (gnutella-svc), 1026 (win-rpc), 4662 (eDonkey2000), 139 (netbios-ssn), 113 (auth), 6881 (bittorrent), 3621 (---), 445 (microsoft-ds), 2234 (directplay), 25 (smtp)
----------------------------	---

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

38. *October 19, CNN* — FBI: 20-year-old suspected of NFL bomb hoax. The FBI and the Department of Homeland Security (DHS) have determined that a threat against NFL stadiums was a hoax, FBI spokesperson Richard Kolko told CNN Thursday, October 19. Earlier, the FBI interviewed and released a Milwaukee man after his friend came forward with information about the online posting of a threat against NFL stadiums. The FBI told CNN that agents do not believe the man has any connections to terrorism, but do believe the 20-year-old was involved in making the threat. DHS this week sent an advisory to the National Football League and local officials describing a possible uncorroborated threat against some NFL stadiums. The threat, posted on a Website, alleged that bombs could be used this weekend against stadiums in Miami, New York, Atlanta, Seattle, Houston, Oakland, and Cleveland. The posting said the bombs were to be delivered by truck. The DHS said earlier the posting was not considered credible, and that the information was being shared only out of caution so that league officials and others could determine what steps to take.

Source: <http://www.cnn.com/2006/US/10/19/nfl.threat/index.html>

[\[Return to top\]](#)

General Sector

Nothing to report.

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:
<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.